

UNITED STATES DISTRICT COURT

for the
District of South Dakota

IN THE MATTER OF THE SEARCH OF:)

The premises known as the offices of)

Dropbox, Inc., 333 Brannan Street)

San Francisco, CA 94107)

legalcompliance@dropbox.com)

Email addresses:)

Daxm200017@gmail.com; Js2013@gmail.com;)

troynunya@gmail.com;)

hammers2269@gmail.com; and)

lettschase@gmail.com.

Case No. 5:20-mj-144

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. §§ 2252 and 2252A

Offense Description
 Receipt and Possession of Child Pornography

The application is based on these facts:

- ☒ Continued on the attached affidavit, which is incorporated by reference.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.
☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.
☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

Applicant's signature



Special Agent Stephen Berry, FBI
Printed name and title

Sworn to before me and: ☐ signed in my presence.

☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: 7/24/20



Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

Case No. **5:20-mj-144**

CC: AUSA Sazama and Agent

Case No.:

Date and time warrant executed:

Inventory made in the presence of:

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

IN THE MATTER OF THE SEARCH OF: CR

The premises known as the offices of
Dropbox, Inc., 333 Brannan Street
San Francisco, CA 94107
legalcompliance@dropbox.com

**AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT
APPLICATION**

Email addresses:

Daxm200017@gmail.com;
Jsy2013@gmail.com;
troynunya@gmail.com;
hammers2269@gmail.com; and
lettschase@gmail.com

REDACTED

State of South Dakota)
) ss
County of Pennington)

I, Stephen Beery, being duly sworn, states as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Rapid City, South Dakota, office. I have been employed as a Special Agent for the FBI since May 2016. As part of my duties, I investigate violations of federal law, including the online exploitation of children and the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have gained expertise in conducting investigations involving the sexual exploitation of minors and the production and sharing of material depicting their exploitation through training programs, classwork, and investigative work related to conducting these types of investigations, and I have observed and reviewed numerous examples of child

pornography in a variety of media. I have furthermore participated in the execution of numerous federal and state search warrants, which involved the sexual exploitation of children and/or child pornography offenses.

2. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of federal law to include United States Statutes 18 U.S.C. §§ 2251, 2252, and 2252A, involving violations of law involving child pornography. During my law enforcement-career, I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

3. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals, including other law enforcement officers, interviews of persons with knowledge, my review of documents, interview reports and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, I have not

withheld information known to me that would tend to negate probable cause has been withheld from this affidavit.

4. I make this affidavit in support of an application for a search warrant for information associated with the accounts of Daxm200017@gmail.com; Jsy2013@gmail.com; troynunya@gmail.com; hammers2269@gmail.com; and lettschase@gmail.com that are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107 hereinafter referred to as “premises,” and further described in Attachment A hereto.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2251, 2252, and 2252A, relating to material involving the sexual exploitation of minors.

- a. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.
- b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced

using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

DROPBOX INC.

6. “Dropbox” refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an “offsite” storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual’s computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

7. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for

paying subscribers, means and source of payment (including any credit or bank account number).

8. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

9. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

10. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND OF THE INVESTIGATION

11. On February 20, 2020, I received information from the FBI Violent Crimes Against Children squad in Salt Lake City, Utah, that during an undercover operation, agents observed a LiveMe user posting links to child pornography. LiveMe is a social media application which operates solely on the internet. Preliminary investigation to attempt to identify the LiveMe user revealed the user had an address in Rapid City, South Dakota. The user, later identified as 38-year-old Jebadiah Stephen Swenson, utilized LiveMe user number LM-259612291.

12. Agents served a subpoena on Live.me for account information associated with user number LM-259612291 and email swensonjeb04@gmail.com. Live.me returned information associating that account with several IP addresses and with the email address swensonjeb04@gmail.com.

13. Agents served a subpoena on Verizon Wireless for information regarding several "natting" IP addresses linked to the images of child

pornography observed during the undercover activity referenced in paragraph 11. Unlike IP addresses assigned to a specific location, “natting” IP addresses are for mobile users and allows multiple users to utilize the same IP address at the same time. The subpoena sought information for phone number (605) 389-6667, a phone number that had been using several of the natting IP addresses.

14. Agents issued a subpoena to Google for username swensonjeb04. Google responded that the user was “Jeb Swenson,” with account recovery phone number (605) 389-6667, the same phone number associated with the natting Verizon IP addresses. The return also revealed the user had Google ID 721317720333 and recovery email address swensjeb04@gmail.com.

15. Agents issued two separate search warrants to Google for the contents of and information associated with the accounts swensonjeb04@gmail.com and swensjeb04@gmail.com, respectively.

16. Agents issued a search warrant to LiveMe for the contents of and information associated with LiveMe account LM-259612291, associated with the email address swensonjeb04@gmail.com.

17. Agents issued a subpoena to Clarity Telecom/Vast Broadband for another IP address associated with the images of child pornography observed during the undercover activity referenced in paragraph 11. Vast Broadband identified the user of the IP address as Autumn Swenson, [REDACTED], Rapid City, South Dakota 57701. I identified Autumn Swenson as Jebadiah Swenson’s wife.

18. I surveilled the residence at [REDACTED], Rapid City, South Dakota 57701, and determined it appears Jebadiah Swenson resides at that location.

19. On April 13, 2020, I received from Google a collection of four zip files containing user content, pursuant to the search warrant served on Google, Inc. for content associated with user swensonjeb04.

20. One of the zip files I received from Google contained several photo files and folders. In a folder in the photo zip file entitled "2019-06-27," I observed images matching the LiveMe user profile picture observed during the undercover activity referenced in paragraph 11.

21. In a folder entitled "2019-12-18", I observed an image entitled "Screenshot_20191218-185850_TamTam.jpg." This image is an image of child pornography. The image depicts a nude adult female on her back with legs open. A nude minor female, approximately 7 years of age, is kneeling in front and inserting her entire hand into the adult female's vagina.

22. In a folder entitled "2020-01-22," I observed images of the phone owner's face and body. This person appears to be Jebadiah Swenson.

23. In a folder entitled "2020-01-24," I observed two images of child pornography. The files appear to be screenshots taken from the UNICO LIVE app, a video streaming application. The images contain a minor female touching and exposing her vagina to the camera in a sexual pose.

24. One of the zip files contained email content. In the “email” file, I observed an email sent on September 25, 2019, from swensonjeb04@gmail.com to the LiveMe application, asking the LiveMe application to reinstate his user account, “lovethemhotones20,” which had been banned.

25. Several usernames for various platforms were identified in the Google “email” file: Facebook username “swensonjeb04@gmail.com”; Snapchat username “jebswenson19”; and eBay username “jeswenso2.”

26. I received and reviewed the search warrant return from LiveMe. The user LM-259612291 engaged in multiple chats using the LiveMe application between the dates October 1, 2019, and March 7, 2020. Several of the messages expressed interest in receiving links from other users and referenced “11-16?” which appears in the context of the messages to be seeking links for images or files of children aged 11 to 16. The messages also contained conversations about trading links or files.

27. On June 2, 2020, agents executed a search warrant on the property located at [REDACTED], Rapid City, South Dakota 57701, and to search any curtilage, storage units, persons and vehicles on the premises and associated with the property, as well as the content of any computer and electronic storage devices located on the property or on the person of Jebadiah Swenson.

28. Seized pursuant to the execution of the aforementioned search warrant on the property located at [REDACTED] was, among other devices, a black Samsung Galaxy S7 Edge cellular phone.

29. During the search of the black Samsung Galaxy S7 Edge cellular phone, your affiant observed several hundred images on the cellular phone depicting child sexual abuse. Your affiant also observed several Google accounts that were then logged into or had previously been logged into on the cellular phone, including Daxm200017@gmail.com; Jsy2013@gmail.com; troynunya@gmail.com; hammers2269@gmail.com; and lettschase@gmail.com.

30. Your affiant also observed the Dropbox app present on the device. Though the phone was offline, a thumbnail of a video present on the account was stored on the device. The title of the video was “pthc_pedo Cerdo de mired...o de nene de 10 anitos.flv”. In your affiant's experience, “pthc” stands for “pre-teen hardcore”, “pedo” is short for pedophilia, and 10 anitos is spanish for 10-year-old. During further review of the device, your affiant discovered several email addresses associated with Dropbox, including Daxm200017@gmail.com; Jsy2013@gmail.com; troynunya@gmail.com; hammers2269@gmail.com; and lettschase@gmail.com.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL
INTEREST IN CHILDREN AND/OR WHO RECEIVE AND/OR POSSESS
CHILD PORNOGRAPHY**

31. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law

enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

- a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs,

correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. The user often maintains these child pornography images for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time-period. Law enforcement officers involved in the investigation of child pornography throughout the world have documented this behavior. Thus, even if the unknown user uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found within the SUBJECT ACCOUNT.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

32. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require DropBox, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

33. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a “district court of the United States (including a magistrate judge of such court)” that “has

jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

REQUEST/JUSTIFICATION FOR ORDER OF NONDISCLOSURE

34. The United States respectfully applies for an order of nondisclosure to DropBox, Inc. under 18 U.S.C. § 2705(b) regarding the following accounts: Daxm200017@gmail.com; Jsy2013@gmail.com; troynunya@gmail.com; hammers2269@gmail.com; and lettschase@gmail.com. The United States is seeking this search warrant for subscriber information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding DropBox, Inc. not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the order of nondisclosure if the court determines the notification to the subscriber could result in one of the five factors listed in the statute, which includes destruction of or tampering with evidence. 18 U.S.C. § 2705(b)(3). The basis for the request is that such disclosure could cause any person with access to the accounts, or any related account or account information, to tamper with or modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to DropBox, Inc., persons can

modify its content with internet access and sufficient account information. As such, the United States respectfully requests this Court enter an order commanding Google, Inc. not to notify the user of the existence of this warrant.

LIMIT ON SCOPE OF SEARCH

35. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

REQUEST FOR SEALING OF MATTER

36. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

CONCLUSION

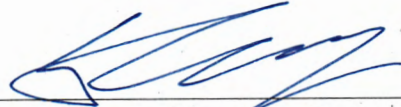
37. Based on the aforementioned factual information, your Affiant respectfully submits this Affidavit in support of probable cause for a Warrant to search the location described in Attachment A and seize the items described in Attachment B which are in violation of 18 U.S.C. § 2252A including items of instrumentality for those crimes.

RETURN COMPLIANCE BY DROPBOX, INC.

38. DropBox, Inc.'s policies prohibit mailing or emailing child pornography to law enforcement in response to a search warrant, instead requiring a law enforcement officer to personally appear and collect contraband materials, unless the means of production is explicitly described in that search warrant. Specifically, DropBox, Inc. requires the Court order the disclosure, notwithstanding 18 U.S.C. § 2252A or similar statute or code.

Dated: _____

7/23/20



Special Agent Stephen Beery
Federal Bureau of Investigation

Sworn to before me and:

☐ signed in my presence.

☒ submitted, attested to, and acknowledged by reliable electronic means.

this 23rd day of July, 2020.



Daneta Wollmann
United States Magistrate Judge

ATTACHMENT A
Location to Be Searched

The property to be searched is the accounts of

- Daxm200017@gmail.com;
- Jsy2013@gmail.com;
- troynunya@gmail.com;
- hammers2269@gmail.com; and
- lettschase@gmail.com

that are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107.

ATTACHMENT B
Items to be Seized

I. Information to be disclosed by Dropbox, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, Inc. including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;
- b. All transactional information of all activity of the Dropbox accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting; and emails “invites” sent or received via Dropbox, and any contact lists.
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A involving the accounts associated with Daxm200017@gmail.com; Jsy2013@gmail.com; troynunya@gmail.com; hammers2269@gmail.com; and lettschase@gmail.com pertaining to the possession and distribution of child pornography images and/or child exploitation material.

III. Method of delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to the Special Agent designated on the fax cover sheet located at the address

Special Agent Stephen Beery
3600 Jet Drive, Rapid City, SD 57703
605-872-4114
sbeery@fbi.gov

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL
RULE OF EVIDENCE 902(11) and (13)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by DropBox, Inc., and my official title is _____. I am a custodian of records for DropBox, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of DropBox, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of DropBox, Inc.; and

c. such records were made by DropBox, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature